Algorithms for and against the Cloud

Roger Wattenhofer
Disclaimer
Algorithms for the Cloud
Algorithms for the Cloud Infrastructure
Algorithms for the Cloud

just perfect
Algorithms for the Cloud
Find balanced separator of minimum size $K$. 
Find balanced separator of minimum size $K$. 

[NP-hard] [Bui and Jones, 1992]
Find balanced separator of minimum size $K$. 

Approx. [Feige, Mahdian, 2006] 

NP-hard [Bui and Jones, 1992]
Find balanced separator of minimum size $K$.

Our result: almost linear time algorithm for small $K$.

[Brandt, W., 2017]
Find balanced separator of minimum size $K$.

Our result: almost linear time algorithm for small $K$...in a boring way

[Brandt, W., 2017]
Algorithms for the Cloud

just perfect
GPS for the Cloud
Just record 1ms of raw data
Coarse Time Navigation

Exhaustive Search in Area
Also Robust to GPS Spoofing
Algorithms for the Cloud

just perfect
$100B Revenue

$\frac{3}{4}$ Online
Online Two Player Games

Match Players Fast
Waiting is Booooor/{{$i}}ng
Match Players Well
Similar Rating, Location, etc.
Min-Cost Perfect Matching With Delays (MPMD)
MPMD Example

time

rating (space)
MPMD Example
MPMD Example

rating (space)

time

•

•
MPMD Example

rating (space)

time
MPMD Example

rating (space)

time

space cost

time cost
MPMD Example

rating (space)

time

time cost

space cost
MPMD Example

time

rating
(space)

space cost

time cost
Haste Makes Waste!
MPMD Example

diagram with points labeled 'time cost' and 'space cost' on a graph with axes labeled 'rating (space)' and 'time'.
MPMD Example
Online Matching Literature

- Bipartite graph, left side is known, right side revealed online
  - Maximum cardinality matching
  - Maximum vertex weighted matching
    [AGKM2011, DJK2013, NW2015]
  - Maximum capacitated assignment (the AdWords problem)
  - Metric maximum weight matching
    [KP1993, KMV1994]
  - Metric minimum cost perfect matching
    [KP1993, MNP2006, BBGN2014]
  - Metric minimum capacitated assignment (transportation)
    [KP2000]
- MPMD: known graph, both sides revealed online
MPMD Results

- Finite metric space $\mathcal{M} = (V, \delta)$
  - $n = |V|$
  - $\Delta = \frac{\max_{x \neq y \in V} \delta(x, y)}{\min_{x \neq y \in V} \delta(x, y)}$

- $O(\log^2 n + \log \Delta)$-competitive randomized algorithm
  [Emek, Kutten, W 2016]

- $O(\log n)$-competitive (almost) deterministic algorithm
  Lower bound of $\Omega(\sqrt{\log n})$
  [Azar, Chiplunkar, Kaplan 2017]

- $O(\log n)$-competitive (almost) det. bipartite algorithm
  $\Omega(\sqrt{\log n / \log \log n})$ lower bound for bipartite
  $\Omega(\log n / \log \log n)$ lower bound for non-bipartite
  [Wang et al., 2018]

...
The $O(\log n)$ Algorithm
Approximate Metric by Tree

Leaves = Nodes in Metric Space

Height = $O(\log n)$
$E[\text{Distortion}] = O(\log n)$

Algorithm
Algorithm
Algorithm
Algorithm
Algorithm
Proof
Proof

Total space cost = $\sum$
Proof
Proof
Proof

For each pair at least one timer running

Total time cost \( \leq 2 \sum \)
Total Algorithm Cost = $O\left(\sum \text{\textcolor{red}{\textbullet}}\right)$
What about OPT?
Proof
Proof
Proof
Proof

or
Proof

\begin{equation}
\text{cost} = \text{cost}
\end{equation}
Done?
Just One Little Thing...
Proof
Proof
Proof
Proof
Proof
Proof
Proof
Proof
OPT has an easy time...
... but only every other phase!
Total OPT Cost $= \Omega (\sum \times)$
Where is the $\log n$ coming from?

Height = $O(\log n)$ for time
$E[\text{Distortion}] = O(\log n)$ for space
AND NOW FOR SOMETHING COMPLETELY DIFFERENT
Algorithms against the Cloud
Will Blockchain Kill the Cloud?

Launch: Introducing Oracle Autonomous Blockchain Cloud Service

The blockchain is here to make cloud computing better

Why Blockchain is Cloud 2.0

BlockCloud: Re-inventing Cloud with Blockchains

FUTURE OF CLOUD COMPUTING IS DECENTRALISED BLOCKCHAIN
CURRENCY OF THE FUTURE?
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis and each node takes part in the validation process.
Blockchain

Figure 9-3  Manual Journal Voucher.

<table>
<thead>
<tr>
<th>Batch</th>
<th>Batch Line</th>
<th>Description</th>
<th>Total Amount</th>
<th>Preparer</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1101</td>
<td>9</td>
<td>ACCRUED INTEREST INCOME</td>
<td>11,200.20</td>
<td>WLR</td>
<td>2/18/18</td>
</tr>
</tbody>
</table>

Reference: JY3-JAN INTEREST

Accounting Company: ID-CORPORATE

<table>
<thead>
<tr>
<th>Seq</th>
<th>Account Number</th>
<th>Description</th>
<th>Debit Amount</th>
<th>Credit Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>1280-000</td>
<td>INTEREST RECEIVABLE</td>
<td>11,200.20</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>8050-010</td>
<td>FIRST NATIONAL - CD</td>
<td></td>
<td>1,330.10</td>
</tr>
<tr>
<td>03</td>
<td>8050-030</td>
<td>MUNICIPAL BONDS</td>
<td>6,220.80</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>8050-010</td>
<td>OTHER INVESTMENTS</td>
<td>3,649.30</td>
<td></td>
</tr>
</tbody>
</table>
FinTech developers and managers understand that the blockchain has the potential to disrupt the financial world. The blockchain allows the participants of a distributed system to agree on a common view of the system, to track changes in the system, in a reliable way. In the distributed systems community, agreement techniques have been known long before cryptocurrencies such as Bitcoin (where the term blockchain is borrowed) emerged. Various concepts and protocols exist, each with its own advantages and disadvantages. This book introduces the basic techniques when building fault-tolerant distributed systems, in a scientific way. We will present different protocols and algorithms that allow for fault-tolerant operation, and we will discuss practical systems that implement these techniques.

About the author

Roger Wattenhofer is a professor at ETH Zurich. Before joining ETH Zurich, he was at Brown University and Microsoft Research. His research interests include fault-tolerant distributed systems, efficient network algorithms, and cryptocurrencies such as Bitcoin. He has published more than 250 scientific articles.
Blockchain Basics
Transaction
Transaction
Transaction
Transaction
Block
Blockchain
Blockchain is Replicated
Blockchain

Distributed Systems & Cryptography
Blockchain

Distributed Systems & Cryptography
Fault-Tolerance & Digital Signatures
Rule of Thumb

Blockchains* may disrupt your business if you use signatures.

*or blockchain-like tech
Blockchain Variants
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/20</td>
<td>Rent</td>
<td>$1,200</td>
</tr>
<tr>
<td>2/1/20</td>
<td>Utilities</td>
<td>$250</td>
</tr>
<tr>
<td>3/1/20</td>
<td>Mortgage Payment</td>
<td>$1,500</td>
</tr>
<tr>
<td>4/1/20</td>
<td>Utilities</td>
<td>$200</td>
</tr>
<tr>
<td>5/1/20</td>
<td>Rent</td>
<td>$1,200</td>
</tr>
<tr>
<td>6/1/20</td>
<td>Insurance Payment</td>
<td>$500</td>
</tr>
</tbody>
</table>

**Total: $5,450**
Permissionless / Open
Permissioned / Closed
Multiple Participants?

- No Blockchain (use DB/Cloud)
- Permissionless Blockchain

Writers Known?

- Yes
- No

Permissioned Blockchain

- No
- Yes
The Seven Blockchain Dimensions

Persistence
Privacy
Energy
Fault-Tolerance
Throughput
Speed
Persistence
Energy
Blockchain

Persistence
- Database
- Immutable
- Provable

Fault-Tolerance
- Correct
- Crash
- Byzantine
Blockchain

**Speed**
- 1 hour
- 1 minute
- 1 second

**Throughput**
- 10 tx/s
- 10k tx/s
- 10m tx/s
Blockchain

Scalability

10 nodes

100 nodes

1000 nodes
Energy Consumption
«Ich wäre nicht überrascht, wenn Bitcoin verboten würde»

ETH-Informationstechnologe Roger Wattenhofer über den Energiebedarf der Kryptowährung und bessere Alternativen
Economic Incentives

Market / Energy Value $\approx 12 \text{ GW}$

$1\text{M/h}$  $0.08/\text{kWh}$
Proof of Work

Hashrate \cdot Energy/Hash \approx 1.3 \text{ GW}

13 \cdot 10^9 \text{ GH/s} \quad 0.1 \text{ J/GH}
The Seven Blockchain Dimensions

- Persistence
- Privacy
- Energy
- Fault-Tolerance
- Throughput
- Speed
- Permission
What About Privacy?
It’s Complicated.
Privacy

Anonymity/Public       ←       Identity/Private
Research Issues

Solution to “many” problems: “Layer 2”

Plus: crypto, language (smart contracts), game theory, measurements, ...
Permissioned Blockchain & Payment Network
Permissioned Blockchain
Payment Network
<table>
<thead>
<tr>
<th><strong>Bitcoin</strong></th>
<th><strong>eMoney</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity</td>
<td>Accountability</td>
</tr>
<tr>
<td>Open/Anarchic</td>
<td>Closed/Private</td>
</tr>
<tr>
<td>Blockchain</td>
<td>Paxos, PBFT, ...</td>
</tr>
<tr>
<td>Eventual Consistency</td>
<td>Strong Consistency</td>
</tr>
<tr>
<td>Proof-of-Work</td>
<td>Central Banks</td>
</tr>
</tbody>
</table>
eVoting
What’s Wrong with Paper?
Cost
Verifiability
Anonymity

Identity Swapper
Identity Mixer

...
Election Help
Wie viel sollen die SRG-Gebühren pro Jahr kosten?

42.-
Don’t bring a Blockchain to a Gunfight
So what’s new, really?
Hello World!

Classical Adversary

- timing
- crashes
- omission
- Byzantine

Now solve consensus
Здравствуйте!

Now hold an election

Modern Adversary

meltdown

spectre

re-entrancy

rowhammer
Hype

“First practical solution to a longstanding problem in computer science, Byzantine Generals.”

“Satoshi solved a problem that academic computer scientists thought was impossible”

“Bitcoin is digital gold, it will put us back onto a sound monetary policy”

“Bitcoin will end wars”

... and Criticism

“A non-deliberate Ponzi scheme”

“It’s yet another eventually consistent database”

“Flawed technology, inherently limited in scale and performance”

“Unlikely to impact the finance sector”
Would you rather fight…?

Cloud vs. Blockchain
Would you rather trust...?

big corporation

Cloud vs. Blockchain
Thanks to lots of hardware...

Moving to the cloud can save up to 87% of IT energy.

By moving 86 million U.S. office workers to the cloud, we would use up to 87% less energy. That's enough to power Los Angeles for 1 year.

Cloud vs. Blockchain
“We at big corp will run your blockchain in our cloud!”
What’s this?
A Blockchain?
A Cloud?
A Distributed System!
Summary
Thank You!

Questions & Comments?

Thanks to my co-authors
Vertex Separators: Sebastian Brandt
Online With Delay: Yuval Emek, Shay Kutten
Cloud GPS: Manuel Eichelberger

www.disco.ethz.ch
Abstract:

Algorithms interact in two main ways with the cloud. There exist algorithms which are tailored for the cloud, for which the cloud is the perfect environment. Moreover, the cloud may also benefit from optimization algorithms, algorithms that make the cloud more efficient. The AlgoCloud program features papers which roughly fit one of the two, and I will also give a few examples in the first part of my talk. Apart from these algorithms for the cloud, I will also talk about algorithms against the cloud. Recently, blockchains are hyped to be a cloud competitor, sometimes even a cloud killer. In the second part of my talk we will discuss whether there is some truth to whether blockchains are going to threaten the successful cloud paradigm.